Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

UAC-0099 Utilizes WinRAR Exploit to Deploy LONEPAGE Malware

Date of Publication	Admiralty Code	TA Number
December 28, 2023	A1	TA2023523

Summary

Attack Began: Early August 2023
Attack Region: Ukraine
Actor: UAC-0099
Malware: LONEPAGE
Attack: UAC-0099, a threat actor, has been involved in persistent attacks targeting Ukraine. These attacks leverage a critical vulnerability in WinRAR to deploy a malware strain known as LONEPAGE. Notably, the threat actor focuses on Ukrainian employees working for organizations outside of Ukraine.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-38831	RARLAB WinRAR Code Execution Vulnerability	WinRAR	✓	✓	✓

Attack Details

#1 UAC-0099, a threat actor, has been actively targeting Ukraine since mid-2022, leveraging the vulnerability CVE-2023-38831. They focus on Ukrainian employees working for organizations outside of Ukraine. The group utilizes various infection vectors, including phishing attacks with HTA, RAR, and LNK file attachments. The final-stage malware in these attacks is the Visual Basic Script (VBS) malware LONEPAGE.

#2 The attack orchestrated by UAC-0099 involved phishing messages employing HTA, RAR, and LNK file attachments to distribute LONEPAGE, a VBS malware with capability to establish command-and-control (C2) communications. The infection chain employed three different methods.

#3 The first method involves using HTA Attachments, embedded VBScript is executed to invoke PowerShell. In the second method involving Self-Extracting Archives, a disguised LNK shortcut triggers malicious PowerShell code. An additional attack vector employs a crafted ZIP archive, attempting to exploit CVE-2023-38831 for PowerShell execution. The executed PowerShell script introduces the LONEPAGE malware into the system.

#4 A persistence entry is made for LONEPAGE in Schedule Task, and upon execution, it generates a concealed PowerShell script that communicates with a command-and-control (C2) server for additional instructions. LONEPAGE enables threat actors to execute arbitrary PowerShell code on the compromised computer and receive corresponding responses.

#5 To minimize the risk of UAC-0099 attacks and promptly identify potential compromises, organizations should vigilantly monitor and restrict specific components. It is crucial to address vulnerabilities promptly, considering that multiple threat actors are exploiting the WinRAR flaw, highlighting the importance of timely patching.

Recommendations

Patch or Update WinRAR: Ensure that all instances of WinRAR in your organization are updated to versions 6.23 or higher to address the CVE-2023-38831 vulnerability. Regularly check for updates and automate the patching process where possible.

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Continuous Monitoring: Regularly monitor and audit PowerShell usage and scheduled tasks to promptly identify and investigate any anomalies or suspicious activities.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious content.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0004 Privilege Escalation	**TA0005** Defense Evasion	**TA0009** Collection	**TA0010** Exfiltration
TA0011 Command and Control	**T1547** Boot or Logon Autostart Execution	**T1053** Scheduled Task/Job	**T1059** Command and Scripting Interpreter
T1059.001 PowerShell	**T1059.005** Visual Basic	**T1560** Archive Collected Data	**T1106** Native API
T1176 Browser Extensions	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1036** Masquerading
T1041 Exfiltration Over C2 Channel	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1071** Application Layer Protocol
T1071.001 Web Protocols			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	d21aa84542303ca70b59b53e9de9f092f9001f409158a9d46a5e8ce82ab60fb6, 0eec5a7373b28a991831d9be1e30976ceb057e5b701e732372524f1a50255c7, 8aca535047a3a38a57f80a64d9282ace7a33c54336cd08662409352c23507602, 2c2fa6b9fbb6aa270ba0f49ebb361ebf7d36258e1bdfd825bc2faeb738c487ed, 659abb39eec218de66e2c1d917b22149ead7b743d3fe968ef840ef22318060fd, 0aa794e54c19dbcd5425405e3678ab9bc98fb7ea787684afb962ee22a1c0ab51, 4e8de351db362c519504509df309c7b58b891baf9cb99a3500b92fe0ef772924, 53812d7bdaf5e8e5c1b99b4b9f3d8d3d7726d4c6c23a72fb109132d96ca725c2, 38b49818bb95108187fb4376e9537084062207f91310cdafcb9e4b7aa0d078f9, a10209c10bf373ed682a13dad4ff3aea95f0fdcd48b62168c6441a1c9f06be37, 61a5b971a6b5f9c2b5e9a860c996569da30369ac67108d4b8a71f58311a6e1f1, 86549cf9c343d0533ef80be2f080a7e3c38c77a1dfbde0a2f89048127979ec2a, 762c7289fb016bbcf976bd104bd8da72e17d6d81121a846cd40480dbdd876378, 39d56eab8adfe9eb244914dde42ec7f12f48836d3ba56c479ab21bdbc41025fe, f75f1d4c561fcb013e262b3667982759f215ba7e714c43474755b72ed7f9d01e, 986694cad425c8f566e4e12c104811d4e8b30ce6c4c4d38f919b617b1aa66b05, 54458ebfbe56bc932e75d6d0a5c1222286218a8ef26face40f2a0c0ec2517584, 96ab977f8763762af26bad2b6c501185b25916775b4ed2d18ad66b4c38bd5f0d, 6a638569f831990df48669ca81fec37c6da380dbaaa6432d4407985e809810da, 87291b918218e01cac58ea55472d809d8cdd79266c372aebe9ee593c0f4e3b77, f5f269cf469bf9c9703fe0903cda100acbb4b3e13dbfef6b6ee87a907e5fcd1b,

TYPE	VALUE
SHA256	e34fc4910458e9378ea357baf045e9c0c21515a0b8818a5b36daceb2af464ea0, 2a3da413f9f0554148469ea715f2776ab40e86925fb68cc6279ffc00f4f410dd, 0acd4a9ef18f3fd1ccf440879e768089d4dd2107e1ce19d2a17a59ebed8c7f5d, 6f5f265110490158df91ca8ad429a96f8af69ca30b9e3b0d9c11d4fef74091e8, 736c0128402d83cd3694a5f5bb02072d77385c587311274e3229e9b2fd5c5af7

Patch Details

Update WinRAR version to 6.23 or later versions.

References

https://www.deepinstinct.com/blog/threat-actor-uac-0099-continues-to-target-ukraine

https://www.hivepro.com/threat-advisory/apt28s-tactical-exploitation-of-critical-vulnerabilities/

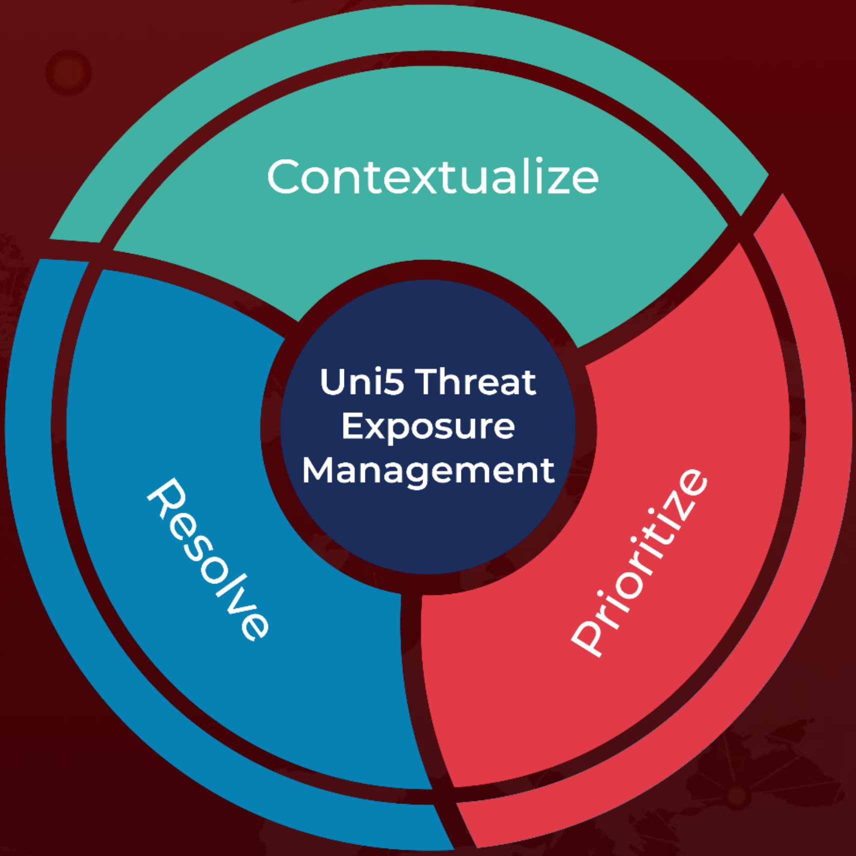
https://www.hivepro.com/threat-advisory/the-rise-of-darkcasino-apt-group-exploiting-winrar-0-day/

https://www.hivepro.com/russian-actors-exploiting-winrar-flaw-cve-2023-38831-in-phishing-attacks/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 28, 2023 • 5:25 AM

More at www.hivepro.com